UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

v.

HOWARD E. BROOKS,

Defendant.

REPORT & RECOMMENDATION

16-CR-6028L

PRELIMINARY STATEMENT

By Order of Hon. David G. Larimer, United States District Judge, dated March 24, 2016, all pretrial matters in the above-captioned case have been referred to this Court pursuant to 28 U.S.C. §§ 636(b)(1)(A)-(B). (Docket # 22). On March 24, 2016, the grand jury returned a six-count indictment charging defendant Howard E. Brooks ("Brooks") with one count of receipt of child pornography, one count of attempted distribution of child pornography, and four counts of possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B). (Docket # 21).

Currently pending before this Court are motions by Brooks to suppress tangible evidence and statements.[1] (Docket ## 31, 47, 54). In a previous report and recommendation, familiarity with which is assumed, this Court concluded that Brooks's motion to suppress statements on the grounds that his *Miranda* rights were violated or that his statements were not

[1] Brooks filed omnibus motions seeking other forms of relief including, *inter alia*, discovery and inspection, Rule 404(b), 608 and 609 evidence, *Jencks* material, preservation of rough notes, and leave to file additional motions. (Docket # 31). Each of the above-referenced motions was decided by the undersigned or resolved by the parties in open court on July 28, 2016. (Docket ## 35, 36).

voluntary should be denied. (Docket # 43). This Court directed the parties to file supplemental memoranda and scheduled a further evidentiary hearing on Brooks's motion to suppress evidence obtained from his computer pursuant to a warrant authorizing the deployment of a Network Investigative Technique ("NIT"). (*Id.* at 23-24).

The parties filed their supplemental memoranda on February 10, 2017, and February 22, 2017. (Docket ## 47-49). The government maintains that the NIT warrant was valid and that the agents relied upon it in good faith; although it had earlier taken a contrary position, the government does not contest that deployment of the NIT constituted a search within the meaning of the Fourth Amendment. (Docket ## 48 at 1; 52 at 3). In support of its supplemental memorandum, the government attached an affidavit from Federal Bureau of Investigation ("FBI") Special Agent Daniel Alfin ("Alfin") addressing questions raised by the Court in its Report and Recommendation. (Docket # 48-1). On April 25, 2017, this Court held an evidentiary hearing at which Alfin testified. (Docket # 51).[2]

For the reasons discussed below, I recommend that the district court deny Brooks's motion to suppress tangible evidence seized during the execution of the NIT warrant. I also recommend that the district court deny Brooks's motion to suppress his statements and the evidence seized from his residence on the grounds that they were the fruit of the execution of the NIT warrant.

FACTUAL BACKGROUND

I. The NIT Warrant

On February 20, 2015, the Hon. Theresa Carroll Buchanan, United States Magistrate Judge for the Eastern District of Virginia, issued a warrant to search property located

[2] The transcript of the evidentiary hearing shall be referred to as "Tr." (Docket # 52).

in the Eastern District of Virginia, which was described in an attachment to the warrant.[3] (Docket # 31 at 31-33). The attachment indicated that the warrant authorized the use of the NIT, a computer code, to be deployed on a computer server operating on the "[Playpen]"[4] website – a child pornography website that was operating on the Tor network (explained in more detail *infra*) and was located at a government facility in the Eastern District of Virginia. (*Id.*). The warrant also authorized the NIT to obtain information from "activating computers," referring to computers of any user or administrator who logged into Playpen by entering a username and password. (*Id.*). The warrant identified the information to be seized as the following:

> 1. the 'activating' computer's actual IP address, and the date and time that the NIT determine[d] what that IP address is;
>
> 2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other 'activating' computers, that [would] be sent with and collected by the NIT;
>
> 3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
>
> 4. information about whether the NIT had already been delivered to the 'activating' computer;
>
> 5. the 'activating' computer's Host Name;
>
> 6. the 'activating' computer's active operating system username; and
>
> 7. the 'activating' computer's media access control ('MAC') address[.]

(*Id.*).

[3] Although my previous decision included a description of the NIT warrant, in the interests of completeness, that description is repeated herein and supplemented by additional relevant information.

[4] The warrant and its supporting materials refer to the website as the "TARGET WEBSITE," although the record before the Court establishes that the website was called "Playpen." (Docket # 34 at 1).

FBI Special Agent Douglas Macfarlane ("Macfarlane") submitted an affidavit in support of the warrant application. (*Id*. at 34-66). Macfarlane's affidavit stated that he had been employed by the FBI since 1996 and had participated in investigations involving child pornography and the sexual exploitation of children. (*Id.* at ¶ 1). According to Macfarlane, the targets of the NIT investigation included the administrators and users of the Playpen website. (*Id.* at ¶ 6). Macfarlane stated that the Playpen website was dedicated to the advertisement and distribution of child pornography, discussions of child sexual abuse, including methods and tactics offenders could use to abuse children and avoid law enforcement detection. (*Id.*). Macfarlane stated that the administrators and users of the Playpen website regularly sent and received illegal child pornography using the website. (*Id.*).

Macfarlane's affidavit explained that the Playpen website operated on the Tor network, which provided anonymity to its users. (*Id.* at ¶ 7). According to Macfarlane, the Tor network was designed by a United States Naval Research Laboratory to protect government communications and is now available to the public. (*Id.*). In order to access the Tor network, a user has to install Tor software. (*Id.*). According to Macfarlane, Tor software protects users' online privacy by routing their communications around a distributed network of relay computers, effectively masking the users' Internet Protocol ("IP") addresses. (*Id.* at ¶ 8). Macfarlane explained that when a user connects through the Tor network, the user's IP address listed in the monitored website's IP address log is the IP address associated with the last computer through which a user's communications were routed (the "exit node") instead of the user's actual IP address, a feature that impedes any ability to trace the Tor user's actual IP address. (*Id.*).

According to Macfarlane, the Playpen website was a "hidden service" that existed on the Tor network. (*Id.* at ¶ 10). A user could access the website only if he or she were using

the Tor network and knew the specific address of the website. (*Id.*). Macfarlane explained that the website would not be found by conducting a "Google search" for the name of the website. (*Id.*). Rather, the user would have to obtain the web address from another user of the site or from internet postings describing the type of content available on the site and identifying the site's address. (*Id.*). Macfarlane opined that, considering the affirmative steps required to access the site, a user would be "extremely unlikely . . . [to] stumble upon the [Playpen] website without understanding its purpose and content." (*Id.*).

Macfarlane stated that between September 16, 2014, and February 3, 2015, FBI agents connected to the internet using the Tor browser and accessed the Tor hidden service for the Playpen website at its Uniform Resource Locater ("URL") muff7i44irws3mwu.onion.[5] (*Id.* at ¶ 11). After arriving at the Playpen website, the screen displayed "images of prepubescent females partially clothed and whose legs [were] spread" and "instructions for joining the site before one [could] enter." (*Id.* at ¶¶ 10, 12). The main page also contained the following text: "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." (*Id.* at ¶ 12). According to Macfarlane, based on his training and experience, he understood the phrase "no cross-board reposts" to mean that the website prohibited "re-posting" material from other websites to the Playpen website and ".7z" to refer to a preferred method for compressing large files or sets of files for distribution. (*Id.*).

According to Macfarlane, two data-entry fields with a corresponding "Login" button appeared to the right of the site name. (*Id.*). The following text appeared below the fields: "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' (a hyperlink to the registration page) with [Playpen]." (*Id.*). Macfarlane

[5] Macfarlane stated that as of February 18, 2015, the URL of the Playpen website had changed, but he accessed the website at the new URL and determined that its content had not changed. (*Id.* at ¶ 11 n.3).

stated that upon clicking the "register an account" hyperlink, the following message was displayed:

> VERY IMPORTANT. READ ALL OF THIS PLEASE.
>
> I will add to this as needed.
>
> The software we use for this forum requires that new users enter an email address, and checks that what you enter looks approximately valid. We can't turn this off but the forum operators do NOT want you to enter a real address, just something that matches the xxx@yyy.zzz pattern. No confirmation email will be sent. This board has been intentionally configured so that it WILL NOT SEND EMAIL, EVER. Do not forget your password, you won't be able to recover it.
>
> After you register and login to this forum you will be able to fill out a detailed profile. For your security you should not post information here that can be used to identify you.
>
> Spam, flooding, advertisements, chain letters, pyramid schemes, and solicitations are forbidden on this forum.
>
> Note that it is impossible for the staff or the owners of this forum to confirm the true identity of users or monitor in realtime all messages posted, and as such we are not responsible for the content posted by those users. You remain solely responsible for the content of your posted messages.
>
> The forum software places a cookie, a text file containing bits of information (such as your username and password), in your browser's cache. This is ONLY used to keep you logged in/out. This website is not able to see your IP and can not collect or send any other form of information to your computer except what you expressly upload. For your own security when browsing o[n] Tor we also recommend that you turn off javascript and disable sending of the "refer[r]er" header

(*Id.* at ¶ 13).

According to Macfarlane, after accepting the terms stated above, in order to complete registration, the user was required to enter a username, password, and email account, although a valid email account was not actually required. (*Id.* at ¶ 14). After registering and

logging into the site, the user would see a list of sections, forums, and sub-forums. (*Id.*). Some of the listed sections appeared to relate to the use of the Playpen website and included topics such as Playpen information and rules, "how to," security and technology, and "general discussion." (*Id.*). Other sections included topics such as "jailbait videos," "jailbait photos," "pre-teen videos," "pre-teen photos," "webcams," "potpourri," "kinky fetish," "other languages," and "stories." (*Id.*). The content of the majority of these sections included discussions of, and images that appeared to depict, child pornography and child erotica. (*Id.* at ¶ 18).

Some of the sections listed sub-forums categorized by "girls" or "boys" and the abbreviations "HC," "SC," and "NN." (*Id.* at ¶ 14). According to Macfarlane, "HC" meant "hardcore" and referred to depictions of penetrative sexually explicit conduct, "SC" referred to "softcore" and referred to depictions of non-penetrative sexually explicit conduct, and "NN" referred to "non-nude," which included depictions of fully or partially clothed subjects. (*Id.* at ¶ 14 and n.5).

Macfarlane stated that the website contained another section and forum that allowed members to exchange their usernames. (*Id.* at ¶ 15). According to Macfarlane, based upon his training and experience, this service was commonly used by individuals engaged in online sexual exploitation of children. (*Id.*). Macfarlane further stated that the website also contained a private messaging feature that allowed users to send private messages to each other. (*Id.* at ¶ 20). Based upon his training, experience and review of the site, Macfarlane believed that the private messaging feature was used to communicate about the dissemination of child pornography and to permit users to identify other users. (*Id.* at ¶ 22). The Playpen website also had features that permitted users to chat with each other and to upload images and videos of child pornography that would be accessible to other users of the site. (*Id.* at ¶¶ 23-25).

In December 2014, the FBI received information from a foreign law enforcement agency that a known IP address appeared to be associated with the Playpen website. (*Id.* at ¶ 28). The FBI investigated the IP address and verified that the Playpen website was hosted from that address. (*Id.*). Through the execution of a search warrant in January 2015, a copy of the server that was assigned to the IP address was seized by the FBI. (*Id.*). FBI agents reviewed the contents of the server and discovered that it contained a copy of the Playpen website. (*Id.*). The FBI maintained a copy of the server containing the Playpen website on a computer facility located at a government facility in Newington, Virginia, located in the Eastern District of Virginia. (*Id.*).

According to Macfarlane, although data from the server provided evidence of criminal activity that had occurred on both the server and the Playpen website, FBI agents were unable to learn the identities of the users and administrators of the Playpen website. (*Id.* at ¶ 29). Macfarlane explained that although some non Tor-based websites have IP address logs that facilitate the location and identification of its users, the Playpen website, by contrast, contained only the IP address associated with the last Tor "exit node" for each user. (*Id.*). Thus, review of the website's logs would not assist law enforcement agents in identifying its users' actual IP addresses, without which their identities and locations could not be determined. (*Id.*).

On February 19, 2015, the FBI executed a search at the residence of the suspected administrator of the Playpen website and thereafter assumed administrative control of the Playpen website. (*Id.* at ¶ 30). According to Macfarlane, the FBI planned to continue to operate the website from the government-controlled server located in the Eastern District of Virginia for a limited period of time in an attempt to identify the administrators and users of the site. (*Id.*). To further that plan, the FBI sought, through Macfarlane's warrant application, judicial

authorization to deploy the NIT to investigate users or administrators who logged onto the Playpen website by entering a username and password. (*Id.* at ¶¶ 31-32). As Macfarlane explained in his affidavit, operation of the NIT would cause the user's computer to transmit certain data to a government-controlled computer that would assist the government in ascertaining the users' identities. (*Id.* at ¶ 33).

Towards the end of his affidavit, under a section entitled "Search Authorization Requests," Macfarlane stated:

> Accordingly, it is respectfully requested that this Court issue a search warrant authorizing the following:
>
> a. the NIT may cause an activating computer – *wherever located* – to send a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer.

(*Id.* at ¶ 46 (emphasis added)).

II. Warrant for 116 Lexington Avenue

On July 13, 2015, United States Magistrate Judge Jonathan W. Feldman issued a search warrant authorizing the search of 116 Lexington Avenue, Elmira, New York. (Docket # 31 at 70-76). Christopher S. Mayfield ("Mayfield"), a Special Agent with the FBI, submitted an affidavit in support of the application for the warrant. (*Id.* at 77-98).

In his affidavit, Mayfield summarized information included in the application for the NIT warrant, including information about the Playpen website, how it operated on the Tor network, the observed content of the website, and details on the steps required to access the website. (*Id.* at ¶¶ 6-20). Additionally, Mayfield described the seizure of the website and the

subsequent deployment of the NIT in order to obtain identifying information concerning the users of the Playpen website. (*Id.* at ¶¶ 21-23).

As Mayfield explained, monitoring of the Playpen website revealed that an account with the username "MogisSlaughter" was originally registered with the Playpen website on August 30, 2014. (*Id.* at ¶ 25). The profile information associated with this account indicated that this user was a "Newbie Member" of the Playpen website and had actively logged into the website for a total of approximately thirty-two hours between August 30, 2014, and March 5, 2015. (*Id.*).

Through the deployment of the NIT, the FBI learned that MogisSlaughter accessed the Playpen website on February 28, 2015, from IP address 74.69.176.140. (*Id.* at ¶¶ 26-27). In addition to the IP address, the NIT also retrieved information indicating that the computer associated with the IP address when it accessed the Playpen website was named "Ed-PC" and that the username associated with the computer was "Ed." (*Id.* at ¶¶ 27, 39). After logging into the Playpen website, the MogisSlaughter user accessed a post entitled "9yo Boy taking cock in his throat & ass." (*Id.* at ¶ 27). According to Mayfield, this post contained a link to, among other things, a video entitled "Black Beauty.7z," with the description "Lil Black Guy Taking hard cock in his throat & asshole." (*Id.*).

Although the account associated with username MogisSlaughter logged into the Playpen website on subsequent occasions, the IP address information was not collected during the subsequent sessions. (*Id.* at ¶ 28). Mayfield described the link titles and substance of other child pornography content accessed by MogisSlaughter while logged into the Playpen website on these other occasions. (*Id.* at ¶¶ 28-31).

FBI agents determined that the IP address associated with the MogisSlaughter account was operated by Time Warner Cable. (*Id.* at ¶ 32). In March 2015, a subpoena was served on Time Warner Cable requesting information relating to the subscriber of the IP address. (*Id.* at ¶ 33). Information received from Time Warner identified the subscriber as Cynthia Brooks with an address of 116 Lexington Avenue, Elmira, New York. (*Id.*). Additional public records research indicated that Ms. Brooks owned the premises and that Howard Edward Brooks III was a possible occupant. (*Id.* at ¶ 35). Surveillance conducted at the premises on June 25, 2015, revealed two vehicles parked in the driveway. (*Id.* at ¶ 40). One of those vehicles was registered to Cynthia Brooks; the other was registered to Howard E. Brooks. (*Id.*).

III. Alfin's Testimony

Alfin testified that he was employed as a Special Agent with the FBI and was currently assigned to the Criminal Investigative Division, Violent Crimes Against Children Section, Major Case Coordination Unit, which was located in Maryland. (Tr. 6). Alfin's responsibilities included investigating individuals who use technology to facilitate the production, advertisement, and distribution of child pornography. (*Id.*). Alfin has taken various courses regarding child pornography investigations and is certified to instruct other law enforcement officers in conducting such investigations. (Tr. 7). Alfin has also received training in computer coding and other technical network and computer-related topics. (Tr. 49).

Alfin testified that he was the case agent for the investigation into "Playpen," a website dedicated to the advertisement and distribution of child pornography that was created in approximately August 2014. (Tr. 8, 16-17). Prior to describing the operation of the Playpen website, Alfin testified about the manner in which individuals access content on a regular

internet website. (Tr. 9). Typically, a user accesses content by using a web browser such as Internet Explorer, Google Chrome, or Firefox. (*Id.*). To access a particular website, the individual types in the URL associated with that website, which causes the user's computer, through its internet provider, to communicate with the computer that is running the website. (Tr. 9-10). Through this communication, the website obtains certain information, including the user's IP address and physical location, and the user obtains information about the website, including its owner and physical location. (Tr. 10). Once a law enforcement officer obtains a user's IP address, he or she is typically able to identify the subscriber's name and location by subpoenaing subscriber information from the internet service provider. (Tr. 38-39).

According to Alfin, use of the Tor network alters the communication process described above. (Tr. 10). The Tor network is comprised of a series of thousands of computers (or "nodes") operating on top of the regular internet. (Tr. 10, 13-14). In order to use the Tor network, a user must first download the Tor browser software and use that program to connect to the internet. (Tr. 10-11). With the use of the Tor browser, the user does not communicate directly with the website; rather, the communications are routed through multiple computers (nodes) running the Tor software and located throughout the world. (*Id.*). Although the user's IP address is communicated to the first node it accesses, the website contacted will see only the IP address associated with the last or exit node through which the communication is routed. (Tr. 11, 15-16). This system permits the user to browse the internet anonymously. (Tr. 11). Alfin testified that use of the Tor network is not unlawful. (Tr. 55, 57).

In addition to permitting anonymous browsing of the internet, the Tor network also provides "hidden services" that permit users to host websites that can be accessed by individuals without revealing the location information for the website. (Tr. 12-13). Tor hidden

services are not accessible through regular browsers. (Tr. 13). In contrast to URLs for regular websites, URLs for Tor hidden services consist of sixteen randomly generated characters and end in ".onion" rather than ".com" or ".net." (Tr. 16). Accordingly, in order to access a hidden service website, the user must either know and type in the lengthy URL or search for a link to that website. (Tr. 16, 19). To connect with a hidden service website hosted by Tor, the user communicates through an even greater number of nodes than when a Tor user connects with a website on the regular internet. (Tr. 76).

Alfin testified that the Playpen website was a Tor hidden service, which had a URL of "UPF45JV3BZIUCTML.onion." (Tr. 26-27). Alfin discovered the website because it was advertised on a separate Tor hidden service containing links to child pornography websites. (Tr. 17). According to Alfin, the initial landing page for the Playpen website depicted two prepubescent females depicted in a sexually suggestive manner wearing either bathing suits or underwear.[6] (Tr. 80-81). Alfin observed the website to be a message-board-style website dedicated to the advertisement and distribution of child pornography. (Tr. 17-18). According to Alfin, there were no sections devoted to non-child exploitation related materials, although some of the photographs posted on the website did not technically constitute child pornography. (Tr. 18, 53). Alfin testified that some of the posts may have included a series of photographs in which the first few pictures depicted non-pornographic images of children. (Tr. 53).

Alfin testified that he believed, based upon his training and experience, that an individual would be "incredibly unlikely" to unintentionally "stumble upon" the Playpen website. (Tr. 18). Alfin explained that an individual first would have to download the Tor software to his or her computer and then obtain the URL address for Playpen from someone else

[6] Alfin testified that the image on the landing page changed during the evening hours of February 19, 2015, shortly before the NIT warrant issued, to an image depicting a single prepubescent girl. (Tr. 78-79).

or search the internet to find a directory providing the links to different Tor child pornography hidden services sites. (Tr. 18-19). In order to access the website's content, an individual then would have to log into the website using either an existing username and password or would have to create a new account. (Tr. 20).

After discovering the website, Alfin documented its content and led the investigative efforts to identify its location, creator and users. (Tr. 18). Although the locations of Tor hidden services are typically not able to be identified, a misconfiguration in the creation of the Playpen website allowed law enforcement to discover that it was located in North Carolina. (Tr. 21). Further investigative efforts led to the arrest of the creator of the website and the discovery of the website's server. (Tr. 22-23). By the time the Playpen website was taken offline in March 2015, it had accumulated "hundreds of thousands of users." (Tr. 58).

According to Alfin, although the creator had been arrested and the server seized, the FBI still could not identify the users of the Playpen website due to the nature of the Tor network. (Tr. 23). The FBI took control of the website and operated it for approximately thirteen days from the Eastern District of Virginia. (*Id.*). The investigative team sought the NIT warrant to assist in identifying members of the website. (*Id.*).

Alfin explained the manner in which the NIT computer code attached to information downloaded from the Playpen server by users of the Playpen website in order to identify those users. (Tr. 41, 68). Specifically, the NIT was installed on the Playpen server in Virginia; when a user downloaded content from Playpen, the NIT attached to that information and downloaded into the temporary storage of the user's computer. (Tr. 32, 65, 67). The NIT then forced the computer to communicate information back to the government over the regular internet, permitting the FBI to learn the IP address associated with the computer. (Tr. 37, 75-76).

In addition to the IP address, this information included the host name operating system, active username, media access control ("MAC") address, and a unique identifier associated with the accessing computer. (Tr. 35-37). Of this information, only the IP address and operating system name are typically conveyed when a computer accesses a website through a non-Tor internet browser. (Tr. 48).

The affidavit in support of the application for the NIT warrant was drafted by Macfarlane with significant input and review by Alfin. (Tr. 24, 39). According to Alfin, the investigative team contemplated that the NIT would "travel" beyond the Eastern District of Virginia once it was installed, and the application in support of the warrant was drafted to explicitly state that NIT would cause information to be sent from activating computers "wherever-located," in order to highlight that fact for the issuing judge. (Tr. 40-41).

According to Alfin, the application for the warrant was reviewed by several FBI agents, as well as attorneys with the FBI and the Department of Justice ("DOJ") Child Exploitation and Obscenity Section. (Tr. 24, 42, 84-85). Alfin personally participated in meetings with the attorneys to discuss the warrant. (Tr. 84-85). During those meetings, none of the attorneys expressed the opinion that the warrant was not authorized by Rule 41 of the Federal Rules of Criminal Procedure, although Alfin could not recall whether any issues relating to Rule 41 were "mentioned specifically." (Tr. 85-86). According to Alfin, "the consensus of the meeting[s] was that the warrant was proper." (Tr. 86). He testified that similar warrants had been obtained in other investigations and had not prompted court challenges. (Tr. 87).

The application for the warrant was submitted to and issued by United States Magistrate Judge Theresa Carroll Buchanan in the Eastern District of Virginia. (Tr. 43-44). Alfin testified that subsequent to the issuance of the warrant and the operation of the NIT, he

learned that in September 2013 an acting assistant Attorney General of the DOJ had written to the chair of the Advisory Committee of the Federal Rules of Criminal Procedure regarding amendments to Rule 41(b). (Tr. 79).

After the NIT warrant was issued, the NIT was deployed; it was configured to deploy only after a user logged into their Playpen account, accessed a section of the website, and clicked on an individual post, which would then download the content of that post, along with the NIT, to his or her computer.[7] (Tr. 28-29). Operation of the NIT occurred in less than one second and did not displace any information on the accessing computer. (Tr. 30, 35). The NIT existed only in the temporary storage of the accessing computer, did not leave any data on the accessing computer, and did not permit the FBI to control or access any content on the computer. (Tr. 30-31, 67-69). The NIT was configured to deploy only once with respect to each Playpen user's account. (Tr. 32-34). The NIT was tested at the beginning and at the end of the period the government operated the server to ensure that it was reporting information accurately. (Tr. 73). Alfin testified that he also tested the code on numerous other occasions to ensure accuracy. (*Id.*).

Alfin testified that the NIT was deployed with respect to the Playpen user account name MogisSlaughter after that user accessed a post entitled "9yo boy taking cock in his throat and ass." (Tr. 46). According to Alfin, in his experience the abbreviation "yo" means years old. (*Id.*). That posting contained a link to a video with the description "Lil Black Guy taking hard cock in his throat and asshole." (Tr. 82). Alfin testified that he had seen the images associated with these posts, although he later submitted an affidavit clarifying that he had not viewed those images, but rather had viewed images associated with another posting accessed by

[7] The NIT was configured to deploy immediately upon login for accounts associated with site administrators. (Tr. 51-52).

MogisSlaughter entitled "4 African black boys in a wild orgy," which depicted a prepubescent black male engaged in penetrative sexual activity. (Tr. 82; Docket # 59).

IV. Brooks's Affidavit

In support of his suppression motion, Brooks submitted an affidavit stating that he had an expectation of privacy in the premises located at 116 Lexington Avenue, Elmira, New York. (Docket # 31 at 26, ¶ 2). According to Brooks, he lived at that location with his mother. (*Id.*).

REPORT & RECOMMENDATION

I. Validity of the NIT Warrant

I turn first to Brooks's challenges to the validity of the NIT warrant. Brooks maintains that the NIT warrant was not supported by probable cause, was overbroad, and did not authorize a search of his computer. (Docket ## 31 at 9-15; 54 at 5-8). He also maintains that the NIT warrant was invalid because it was issued in violation of Rule 41 of the Federal Rules of Criminal Procedure. (Docket ## 31 at 15-17; 54 at 3-5).

As noted above, the government has withdrawn its argument that execution of the NIT warrant did not constitute a search within the meaning of the Fourth Amendment. Rather, the government opposes the motion on the grounds that the NIT warrant was valid, supported by probable cause, and not overbroad. (Docket ## 34 at 13-23; 55 at 15-18). Further, the government argues that the warrant complied with Rule 41 and, even if it had not, suppression is not warranted because any such violation was technical and did not prejudice Brooks. (Docket ## 34 at 23-26; 55 at 1-6). Finally, the government maintains that suppression is not warranted

because the agents relied upon the NIT warrant in objective good faith and public policy weighs against suppression. (Docket ## 34 at 26-29; 55 at 6-15).

As an initial matter, the Playpen investigation and execution of the NIT warrant resulted in the identification and arrest of many individuals on child pornography-related crimes. The validity of the NIT warrant has been the subject of numerous defense challenges and dozens of decisions throughout the country. The overwhelming majority of these cases, including two federal appellate court decisions, have declined to suppress evidence gathered pursuant to the NIT warrant, *see, e.g.*, *United States v. Horton*, 863 F.3d 1041, 1052 (8th Cir. 2017); *United States v. Workman*, 863 F.3d 1313, 1321 (10th Cir. 2017), while only a handful of decisions have ordered suppression, *see, e.g.*, *United States v. Levin*, 186 F. Supp. 3d 26, 44 (D. Mass. 2016).[8] I have reviewed and am familiar with the ever-expanding body of caselaw and, with the benefit of the thoughtful and thorough analysis contained in those decisions, I address the specific challenges raised by Brooks.

A. <u>Probable Cause</u>

Brooks maintains that the NIT warrant was not supported by probable cause because Macfarlane's affidavit failed to establish that a visitor to the Playpen site would understand that the site was dedicated to the distribution of child pornography. (Docket # 31 at 9-12). He also maintains that because the NIT deployed upon the accessing of any link

[8] The district court's decision in *United States v. Levin* has been appealed to the First Circuit.

The district courts in *United States v. Croghan*, 209 F. Supp. 3d 1080 (S.D. Iowa 2016), and *United States v. Workman*, 205 F. Supp. 3d 1256 (D. Colo. 2016), also concluded that suppression was warranted, although those determinations were reversed by the Eighth and Tenth Circuits, respectively. The report and recommendation for suppression issued in *United States v. Carlson*, 2017 WL 1535995, *11 (D. Minn. 2017), was adopted in part and rejected in part in light of the Eighth Circuit's decision in *Horton*. *See United States v. Carlson*, 2017 WL 3382309, *8 (D. Minn. 2017). Further, the Tenth Circuit's decision in *Workman* also calls into question the continued validity of the magistrate's recommendation for suppression in *United States v. Arterbury*, 2016 U.S. Dist. LEXIS 67091, *36 (N.D. Okla. 2016), that was adopted by the district court.

contained on the Playpen website, it is possible that the NIT was deployed to computers that accessed only legal images. (Docket # 54 at 5).

The Fourth Amendment to the Constitution provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV; *see also* Fed. R. Crim. P. 41. In *Illinois v. Gates*, 462 U.S. 213 (1983), the Supreme Court affirmed the "totality of the circumstances" test to determine whether a search warrant satisfies the Fourth Amendment's probable cause requirement. According to the Court, the issuing judicial officer must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. at 238. A reviewing court's obligation is merely to determine that the issuing judge had a "'substantial basis for...conclud[ing]' that probable cause existed." *United States v. Smith*, 9 F.3d 1007, 1012 (2d Cir. 1993) (quoting *Gates*, 462 U.S. at 238-39) (internal quotation omitted); *Walczyk v. Rio*, 496 F.3d 139, 157 (2d Cir. 2007) ("a reviewing court must accord considerable deference to the probable cause determination of the issuing magistrate"). Moreover, "resolution of doubtful or marginal cases should be largely determined by the preference to be afforded to warrants." *United States v. Smith*, 9 F.3d at 1012 (citing *Jones v. United States*, 362 U.S. 257, 270 (1960)).

I find that Macfarlane's affidavit in support of the NIT warrant established probable cause to believe that anyone logging into the Playpen website was doing so for the purpose of viewing or distributing child pornography. Although I agree with Brooks that the Playpen login page did not contain images of naked children, it depicted images of two

prepubescent girls who were scantily clad and posed with their legs spread apart. Moreover, the Playpen website operated as a hidden service on the Tor network, with a non-user friendly URL, making the website extremely difficult to arrive at accidentally. Additionally, Playpen's registration process, completion of which was required to access the site, further suggested to prospective users the illicit nature of the site's content. As Macfarlane described, new users were instructed to register using a false email address, warned to avoid posting any information that could be used to identify them, and advised that the website would not have access to the user's IP address. That the website may have contained some non-pornographic images of children does not detract from the probable cause supporting the warrant.

In sum, I conclude that Macfarlane's allegations about the registration process, the suggestive landing page, and the inability to access easily the hidden service, considered together, provided ample probable cause to believe that any users accessing the site did so for the purpose of accessing or distributing child pornography. In reaching this conclusion, I join many other courts who have also found the NIT warrant to be supported by probable cause. *See United States v. Doroshеff*, 2017 WL 1532267, *5 (C.D. Ill. 2017) ("[t]he[] facts set forth in the NIT warrant affidavit supported probable cause"); *United States v. Taylor*, 2017 WL 1437511, *10 (N.D. Ala. 2017) ("[l]ike every other court to address this issue, the court finds that the NIT warrant was supported by sufficient probable cause"); *United States v. Kahler*, 236 F. Supp. 3d 1009, 1022 (E.D. Mich. 2017) ("[w]hen the entirety of the circumstances are considered, it is questionable whether any user could log into Playpen without providing probable cause for law enforcement to believe they intended to view child pornography"); *United States v. McLamb*, 220 F. Supp. 3d 663, 671 (E.D. Va. 2016) ("[g]iven the totality of the circumstances, substantial support underlies the probable cause finding, and the [d]efendant has not shown otherwise");

United States v. Allain, 213 F. Supp. 3d 236, 245 (D. Mass. 2016) ("[c]onsidering the totality of the circumstances – the appearance and content of Playpen, the fact that it was a hidden service on the Tor network, and its registration terms – the magistrate judge had a substantial basis for concluding that the search warrant was supported by probable cause to believe that evidence of criminal conduct would be found on computers used to log into Playpen[;] [w]hile it may not have been a certainty that Playpen registrants intended to access child pornography, there was a fair probability that users who took the time to locate Playpen, and then log in, did so intending to access child pornography"); *United States v. Anzalone*, 208 F. Supp. 3d 358, 366-67 (D. Mass. 2016) ("Macfarlane's affidavit establishes a fair probability that an individual who downloaded a Tor browser, located the Playpen site, entered an email address and password, and logged in, did so with the purpose of accessing child pornography"); *United States v. Jean*, 207 F. Supp. 3d 920, 934 (W.D. Ark. 2016) ("the [c]ourt is well satisfied that the information provided to [the issuing judge] about the contents of the Playpen website, the details of the NIT protocol, and the way that the TOR software and TOR network operated afforded her a substantial basis for determining there was probable cause to believe that Playpen users knew about the contents of the site when they logged in, and did so with the intent to engage in illegal acts"); *United States v. Henderson*, 2016 WL 4549108, *4 (N.D. Cal. 2016) ("[t]he NIT Warrant was supported by substantial probable cause and evidence that the Playpen website was used to host and exchange child pornography"); *United States v. Matish*, 193 F. Supp. 3d 585, 604 (E.D. Va. 2016) ("it was not unreasonable for the magistrate judge to find that Playpen's focus on anonymity, coupled with Playpen's suggestive name, the logo of two prepubescent females partially clothed with their legs spread apart . . . , and the affidavit's description of Playpen's content, endowed the NIT [w]arrant with probable cause"); *United States v. Darby*, 190 F. Supp. 3d 520, 532 (E.D. Va.

2016) ("the information in the affidavit provided substantial evidence in support of the magistrate's finding that there was probable cause to issue the NIT [w]arrant[;] . . . [a]lthough it is not beyond possibility that some of those who logged into Playpen did so without the intention of finding child pornography, probable cause requires a fair probability that a search will uncover evidence, not absolute certainty").

B. Overbreadth/Particularity

As noted above, the Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. AMEND. IV. "Law enforcement agents are thus barred from executing warrants that purport to authorize 'a general, exploratory rummaging in a person's belongings.'" *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 452 (S.D.N.Y. 2013) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). The requirement of particularity is satisfied where the warrant (1) identifies "the specific offense for which the police have established probable cause"; (2) describes the place to be searched; and, (3) specifies "the items to be seized by their relation to designated crimes." *United States v. Galpin*, 720 F.3d 436, 445-46 (2d Cir. 2013) (internal quotation omitted). When a warrant is insufficiently particular, "there is no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary." *Id.* at 446 (quoting *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992)).

Brooks challenges the NIT warrant on the grounds that it was overbroad and insufficiently particular. (Docket ## 31 at 12-14; 54 at 6-8). According to Brooks, by authorizing the search of any computer accessing the Playpen website, the NIT warrant amounted to a general warrant, which allowed "the FBI to search tens of thousands of computers

for which probable cause to search was not established." (Docket # 31 at 13). Brooks also maintains that the government easily could have sought, obtained and executed a more narrow warrant. (*Id.* at 13-14).

Brooks's challenges are unavailing. The number of computers encompassed by the warrant is irrelevant to the particularity analysis. As discussed at length above, probable cause existed to obtain information from *any* computer used to log into the Playpen website, and the warrant specifically identified the places to be searched as the computers of anyone who logged onto Playpen. *See, e.g.*, *United States v. Gaver*, 2017 WL 1134814, *13 (S.D. Ohio 2017) (rejecting argument that the "NIT warrant was an unconstitutional, general warrant that allowed the FBI 'to conduct a massive number of computer searches on unidentified targets in unknown locations[;]' . . . [t]his [c]ourt finds that the NIT warrant sufficiently describes particular places and things to be searched, *i.e.*, the computers of anyone who logged onto the PlayPen website"); *United States v. Kahler*, 236 F. Supp. 3d at 1021 (rejecting argument that the NIT warrant was impermissibly broad because it "'failed to explain how the government planned to avoid searching the activities of innocent computer users[;]' . . . it is questionable whether any user could log into Playpen without providing probable cause for law enforcement to believe they intended to view child pornography"); *United Sates v. Deichert*, 232 F. Supp. 3d 772, 780 (E.D.N.C. 2017) ("the fact that any number of individuals potentially could trigger [execution of the warrant] does not render the NIT warrant any less particular"); *United States v. Allain*, 213 F. Supp. 3d at 247 ("it is irrelevant how many computers were covered by the warrant, given that there was probable cause to search each one"); *United States v. Broy*, 209 F. Supp. 3d 1045, 1051 (C.D. Ill. 2016) ("[t]hat the warrant encompassed a large number of possible computers potentially located in a large number of districts does not mean it suffered from a lack of

particularity; it merely indicates the FBI suspected a large number of users would access [Playpen] from all over the country"); *United States v. Darby*, 190 F. Supp. 3d at 532-33 ("[d]efendant asserts that the warrant was overbroad because it authorized searches of every individual that logged into Playpen, potentially 'tens of thousands of computers'[;] . . . [t]here was probable cause to search the computers of individuals that logged into Playpen[,] . . . [and] the fact that Playpen facilitated rampant criminality does not affect this finding"). Further, Brooks has failed to cite to any authority – and this Court is aware of none – that requires the government to request the narrowest warrant possible to achieve its investigative goals. Because the warrant encompassed those computers for which probable cause to search existed, it was not impermissibly overbroad.[9] *See United States v. Deichert*, 232 F. Supp. 3d at 780 ("the court is aware of no authority, and defendant cites none, to establish what when an investigatory agency can accomplish its goals through a narrower warrant, the Fourth Amendment particularity requirement prohibits it from seeking a broader one"); *Allain*, 213 F. Supp. 3d at 247 ("it is irrelevant that the warrant could have been narrower, given that the warrant as actually issued was sufficiently narrow to limit searches to computers for which there was probable cause to search"); *United States v. Matish*, 193 F. Supp. 3d at 609 ("the fact that the FBI could have and did narrow its search in this case is immaterial, since the warrant was based on probable cause to search any computer logging into the site").

Brooks also maintains that the warrant failed to particularize sufficiently the manner in which the NIT would be deployed. (Docket # 54 at 7-8). According to Brooks, although the warrant authorized deployment of the NIT on the FBI server located in the Eastern

[9] Although the warrant authorized deployment of the NIT to any activating computer that logged into the Playpen website, Alfin's testimony made clear that, with the exception of administrator accounts, the NIT only deployed to an activating computer after the user attempted to access content from the Playpen site. (Tr. 28-29, 51-52).

District of Virginia, Alfin's testimony demonstrated that the NIT was actually deployed on the activating computers. (*Id.*). Brooks maintains that the warrant did not authorize the FBI to install the NIT onto the activating computers. (*Id.*). I disagree. As an initial matter, the plain language of the warrant authorized the use of the NIT to be deployed on the FBI computer server in order to obtain information "from the activating computers," which were any computers used to log into the Playpen website. (Docket # 31 at 30-33). This language alone provided authority to obtain information from any computers logging into the Playpen website.

Further, Macfarlane's affidavit explained in detail how the NIT would operate and specifically stated that the NIT would cause the activating computers to download instructions, which in turn would cause that computer to transmit information to a government-controlled computer. (*Id.* at 57, ¶ 33). In particular, Macfarlane's affidavit requested authorization for the NIT to "cause an activating computer – wherever located – to send" information to a government-owned computer. (*Id.* at 62, ¶ 46(a)). Alfin testified that the affidavit purposefully called attention to the phrase "wherever located" through the use of hyphenation in order to highlight the phrase for the issuing judge. (Tr. 40-41). I conclude that the warrant sufficiently particularized the method of the NIT's deployment and authorized the use of the NIT to obtain information from activating computers "wherever located." *See United States v. Hernandez-Cuellar*, 2017 WL 2297171, *4 (E.D. Tex. 2017) ("[t]he Macfarlane [a]ffidavit (also incorporated by reference in the NIT Warrant) describes in detail the function of the NIT, computers generally, and the particular crimes . . . that the NIT Warrant targets[;] . . . the NIT [w]arrant sufficiently particularizes the place to be searched as 'the activating computers through the NIT deployed on the [Playpen server]' and . . . this description meets constitutional requirements"); *United States v. Taylor*, 2017 WL 1437511 at *11 ("every court to consider this

question has found the NIT search warrant sufficiently particular[;] . . . [t]hough the Constitution does not require elaborate specificity, the court finds it difficult to imagine how much more specific the descriptions of the place to be searched and the items to be seized could have been") (internal quotations and bracket omitted); *United States v. Jean*, 207 F. Supp. 3d at 936 ("the context for what the FBI was seeking – and what the magistrate judge knowingly ordered . . . was authority to search any 'activating computer' – 'wherever located'").

Finally, Brooks maintains that the NIT warrant did not authorize a search of any computer located outside the Eastern District of Virginia. (Docket # 31 at 14). Again, I disagree. Although Brooks is correct that the warrant indicates the location of the property to be searched as the Eastern District of Virginia, Attachment A, which describes the "place to be searched," makes clear that the NIT would be deployed upon a computer server located in the Eastern District of Virginia and would obtain information from any activating computer. Accordingly, I find that the NIT warrant authorized a search of Brooks's computer once he used it to log into the Playpen website. *See United States v. Gaver*, 2017 WL 1134814 at *13 ("Attachment A makes it clear that, although the computer server was located in Virginia, the NIT would operate to obtain information from the activating computers[;] . . . [i]mplicit in this statement is the concept that these 'activating computers' may be located outside of the district") (collecting cases); *United States v. Pawlak*, 237 F. Supp. 3d 460, 465-66 (N.D. Tex. 2017) ("[t]he NIT [w]arrant therefore authorizes the search and seizure of the server operating the Tor Network child pornography website, which is located at a government facility in the Eastern District of Virginia, and the activating computers, wherever located[;] it is not limited in scope to one FBI computer server located in the Eastern District of Virginia"); *United States v. Tran*, 226 F. Supp. 3d 58, 64 (D. Mass. 2016) ("[a] complete, contextual reading of the warrant

demonstrates, as other district courts have found, that the warrant was not geographically limited to activating computers in the Eastern District of Virginia").

C. Authority to Issue Warrant

Brooks maintains that the issuing judge exceeded her jurisdictional limits by authorizing a search of computers located outside the Eastern District of Virginia. (Docket ## 31 at 15-17; 54 at 3-5). According to Brooks, at the time the NIT warrant was issued, Rule 41(b) of the Federal Rules of Criminal Procedure provided only limited exceptions, not applicable here, permitting a magistrate judge to issue a warrant authorizing a search to be conducted in another district.[10] (*Id.*). Because the NIT warrant authorized a search outside the Eastern District of Virginia, and no enumerated exception applied, Brooks maintains that the issuing judge violated Rule 41. (*Id.*). Further, Brooks contends that the violation of the rule was of constitutional magnitude and prejudiced him, warranting suppression. (*Id.*). He also maintains that Alfin's testimony demonstrates that law enforcement agents were either grossly negligent or acted in reckless disregard of the limits of Rule 41(b) when seeking and executing the NIT warrant. (*Id.*).

The government opposes Brooks's motion, maintaining that the NIT operated as a tracking device authorized under Rule 41(b)(4). (Docket ## 34 at 20-23; 55 at 1-6). The government further contends that even if Rule 41 had been violated, such violation was technical in nature and did not prejudice Brooks. (Docket # 34 at 23-26). Finally, the government urges that suppression is not warranted under the good faith exception. (Docket ## 34 at 26-29; 55 at 6-15).

[10] In making this argument, Brooks acknowledges that Rule 41(b) has since been amended to authorize the issuance of warrants like the NIT warrant at issue in this case. *See* Fed. R. Crim. P. 41(b)(6). Specifically, Rule 41(b) was amended effective December 1, 2016 to provide "that in [certain] circumstances a magistrate judge in a district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and seize or copy electronically stored information even when that media or information is or may be located outside of the district." *See* Fed. R. Crim. P. 41(b) advisory committee's note to 2016 amendment.

Rule 41(b) of the Federal Rules of Criminal Procedure authorizes a magistrate judge to "issue a warrant to search for and seize a person or property located within the district." Fed. R. Crim. P. 41(b)(1). At the time the NIT warrant issued, Rule 41(b) identified several exceptions to this jurisdictional limit, one of which related to the installation of tracking devices. *See id.* at 41(b)(4); *see also United States v. Horton*, 863 F.3d at 1047. The government maintains that the NIT warrant falls within the tracking device exception. (Docket ## 34 at 20-23; 55 at 1-6).

Rule 41(b)(4) authorizes a magistrate judge "to issue a warrant to install within the district a tracking device . . . to track the movement of a person or property located within the district, outside the district, or both." Fed. R. Crim. P. 41(b)(4). A tracking device is defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object." *See* Fed. R. Crim. P. 41(a)(2)(E); 18 U.S.C. § 3117(b).

The government reasons that the NIT was akin to a tracking device installed in the Eastern District of Virginia that provided location information for a computer located in the Western District of New York. (Docket ## 34 at 20-23; 55 at 1-6). According to the government, by accessing the Playpen website, Brooks digitally traveled to the server located in the Eastern District of Virginia and, after accessing and downloading child pornography from the Playpen website, downloaded and transported the NIT to the Western District of New York. (*Id.*). The government maintains that the information the NIT caused to be transmitted to the government is similar to the type of information collected by tracking devices. (*Id.*).

Courts throughout the country have grappled with the question whether the scope of Rule 41(b)(4) extends to the NIT warrant. I agree with those courts that have found that the issuance of the NIT warrant was not authorized by the plain language of Rule 41(b)(4). Simply

stated, the NIT was transmitted to an activating computer located in the Western District of New York, and it instructed that computer to relay information to the government. Rather than permitting the tracking of the location of a person or device, the NIT collected information from activating computers that was later used to identify the activating computer and to learn its location. For this reason, in my estimation, the NIT does not qualify as a "tracking device" within the meaning of Rule 41(b)(4). *See, e.g.*, *Horton*, 863 F.3d at 1048 ("[w]e agree with the majority of courts that have reviewed the NIT warrant [,] . . . [and] have concluded that the plain language of Rule 41 and the statutory definition of 'tracking device' do not … support so broad a reading as to encompass the mechanism of the NIT used in this case") (internal quotations omitted); *United States v. Dorosheff*, 2017 WL 1532267 at *6 ("[b]ecause the NIT program initiates a search of computer data and does not track movement, Rule 41(b)(4) does not apply"); *Taylor*, 2017 WL 1437511 at *13 ("Rule 41(b)(4) did not empower the magistrate judge to issue the NIT warrant"); *Gaver*, 2017 WL 1134814 at *9 ("[b]ecause this information goes far beyond providing location information, the NIT is more than just a tracking device; it is a surveillance device[;] . . . [b]ased on the plain language of this Rule, subsection (b)(4) is inapplicable") (internal quotation omitted); *United States v. Perdue*, 237 F. Supp. 3d 471, 476 (N.D. Tex. 2017) ("[a]lthough caselaw suggests that the court is to construe Rule 41(b) broadly, . . . it cannot render it meaningless"); *Kahler*, 236 F. Supp. 3d at 1019-20 ("[the] distinction between discovering the location of an internet user and tracking movement of property illustrates the unsuitability of Rule 41, as it existed at the time of the NIT warrant, for internet investigations[;] [b]ut the unique challenges created by internet investigations do not justify torturing the language of Rule 41(b)(4) to make the warrant lawful *ex post facto*"); *United States v. Dzwonczyk*, 2016 WL 7428390, *7 (D. Neb. 2016) ("[a]pplying these definitions to the facts of

this case, the [c]ourt finds that the NIT is not a tracking device for purposes of the Rule"); *United States v. Vortman*, 2016 WL 7324987, *10 (N.D. Cal. 2016) ("Rule 41(b) was violated because the NIT was not a tracking device and the NIT warrant authorized searches on computers outside the Eastern District of Virginia"); *United States v. Hammond*, 2016 WL 7157762, *4 (N.D. Cal. 2016) ("[a]uthorizing this kind of out-of-district search was beyond the Eastern District of Virginia magistrate judge's authority under Federal Rule of Criminal Procedure 41[(b)(4)]"); *United States v. Owens*, 2016 WL 7053195, *6 (E.D. Wis. 2016) ("[i]n light of the proposed amendment and the plain language of Rule 41(b)[(4)], the [c]ourt concludes that the magistrate judge issued the NIT warrant without jurisdiction in violation of Rule 41(b)"). *But see, e.g.*, *United States v. Austin*, 230 F. Supp. 3d 828, 833 (M.D. Tenn. 2017) ("the [c]ourt concludes that the NIT [w]arrant does not violate Rule 41(b) because it is the computer equivalent of a 'tracking device' and therefore, falls within the provisions of [s]ubsection (4) of Rule 41(b)"); *United States v. Jones*, 230 F. Supp. 3d 819, 825 (S.D. Ohio 2017) ("[o]nce deployed, the NIT functioned in much the same way as a traditional tracking device sending location information back to the agents[;] . . . [t]he language of Rule 41(b)(4) as it was at the time of the NIT warrant was flexible enough to support such an investigatory technique"); *United States v. Sullivan*, 229 F. Supp. 3d 647, 656 (N.D. Ohio 2017) (finding NIT warrant authorized under Rule 41(b)(4)); *United States v. Bee*, 2017 WL 424905, *4 (W.D. Mo.) ("Rule 41(b)(4) is applicable and . . . Magistrate Judge Buchanan possessed the authority to issue the NIT warrant on that basis"), *report and recommendation adopted*, 2017 WL 424889 (N.D. Mo. 2017).

Of course, not every violation of Rule 41(b) mandates suppression. Rather, Rule 41 violations do not warrant suppression unless the violation is of constitutional dimension or "(1) there was 'prejudice' in the sense that the search might not have occurred or would not have

been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision of the Rule." *United States v. Allen*, 169 F. App'x 634, 636 (2d Cir.) (quoting *United States v. Burke*, 517 F.2d 377, 386-87 (2d Cir. 1975)), *cert. denied*, 548 U.S. 913 (2006).

Brooks maintains that the Rule 41(b) violation in this case was of constitutional magnitude and that, in any event, he was prejudiced by the government's flagrant disregard of Rule 41. (Docket ## 31 at 15-16; 54 at 3-5). Contrary to Brooks's contention, nothing in the record suggests that the government deliberately or intentionally disregarded the jurisdictional scope of Rule 41 by applying for and executing the NIT warrant. Rather, Alfin testified at length that attorneys from both the FBI and the DOJ were involved in the warrant's application process and that the general consensus was that the warrant was valid. Additionally, Alfin testified that he was aware that similar warrants had been issued in other investigations without legal challenge, which further led him to believe that the NIT warrant was lawful.

Whether the Rule 41 violation in this case was of constitutional magnitude is a closer question. Indeed, courts throughout the country have reached different conclusions on this issue. *Compare, e.g.*, *Dorosheff*, 2017 WL 1532267 at *6 ("the NIT warrant violated a substantive provision of Rule 41"), *and Taylor*, 2017 WL 1437511 at *14 ("the Rule 41 violation here was constitutional"), *and Gaver*, 2017 WL 1134814 at *9 (holding that magistrate judge lacked authority to issue the NIT warrant rendering it void *ab initio*), *with United States v. Perdue*, 237 F. Supp. 3d at 477-78 (concluding Rule 41 violation was not of constitutional magnitude; "[t]he Fourth Amendment does not address the powers of magistrate judges or district judges, nor does it address whether judges' power extends beyond district boundaries"), *and Deichert*, 232 F. Supp. 3d at 783 ("where the geographic requirements of Rule 41 are not

contained within nor derived from the Fourth Amendment, a violation of any such geographic requirement is not of constitutional import"), *and United States v. Dzwonczyk*, 2016 WL 7428390 at *13 ("the record as a whole demonstrates that, although the NIT warrant was issued in violation of Rule 41(b), that violation was not of constitutional magnitude") (internal quotation omitted), *and United States v. Vortman*, 2016 WL 7324987 at *11 ("the government's violation of Rule 41(b) was technical[;] . . . the NIT warrant complied with the requirements of the Fourth Amendment – it was issued by a neutral magistrate, backed by probable cause, and sufficiently particular"). Most recently, the Eighth Circuit concluded that the Rule 41 violation was of constitutional dimension. *See Horton*, 863 F.3d at 1049 (holding that jurisdictional errors under Rule 41 rose to level of "constitutional infirmity," rendering NIT warrant "void *ab initio*"). Similarly, courts have disagreed as to whether the violation of Rule 41(b) was prejudicial. *Compare Taylor*, 2017 WL 1437511 at *15 ("[t]he issuing magistrate judge could not comply with Rule 41 because it did not empower her to authorize searches outside of her district[;] [defendant], therefore, was prejudiced by the Rule 41(b) violation"), *and United States v. Carlson*, 2017 WL 1535995 at *8 (defendant established Rule 41(b) violation resulted in prejudice; "[defendant] has satisfied his burden to prove that the several searches at issue would not have occurred if there had been compliance with Rule 41(b)"), *with Deichert*, 232 F. Supp. 3d at 784 ("defendant cannot demonstrate that he suffered prejudice due to this mistake since there is no reason to doubt that a magistrate judge in the Eastern District of North Carolina would have issued the same warrant"), *and Vortman*, 2016 WL 7324987 at *11 ("[b]ecause the NIT warrant could have been deployed in a manner entirely consistent with Rule 41(b), the defendant was not prejudiced and suppression of the warrant is not appropriate").

I need not resolve these questions, however, because I conclude that even if the Rule 41 violation were of constitutional significance or prejudiced Brooks, suppression is not warranted. *See, e.g.*, *United States v. Workman*, 863 F.3d at 1317 (assuming without deciding that the magistrate judge lacked authority to issue the NIT warrant and that the resulting search "was unconstitutional or a prejudicial violation of federal law or a federal rule"; determining that *Leon* applies); *United States v. Schuster*, 2017 WL 1154088, *4-5 (S.D. Ohio 2017) (declining to resolve Fourth Amendment issues raised by NIT warrant and analyzing whether agents acted in good faith).

D. Applicability of the Good Faith Exception

Violations of the Fourth Amendment do not necessarily require suppression in every circumstance. *United States v. Rosa*, 626 F.3d 56, 64 (2d Cir. 2010), *cert. denied*, 565 U.S. 1236 (2012). "Indeed, exclusion has always been our last resort, not our first impulse." *Id.* (quoting *Herring v. United States*, 555 U.S. 135, 140 (2009)). This is true, because "searches pursuant to a warrant will rarely require any deep inquiry into reasonableness, for a warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." *United States v. Leon*, 468 U.S. 897, 922 (1984) (internal citation and quotations omitted).

Brooks maintains that the good faith exception cannot be applied to the NIT warrant because it was void at the time of its issuance and further argues that the Second Circuit would be unlikely to agree with the reasoning of the Eighth and Tenth Circuits in *Horton* and *Workman*, both of which held that the good faith exception applies to the NIT warrant.[11]

[11] *Horton* and *Workman* were decided after the parties in this case submitted their post-hearing memoranda. (Docket ## 53-55). On July 26, 2017, the government submitted a letter to the Court addressing the two decisions. (Docket ## 57; 60). Brooks requested and was granted an opportunity to respond to the

(Docket ## 54 at 4-5; 61). Brooks also contends that Alfin's testimony demonstrates that the agents were negligent and reckless in obtaining the NIT warrant, thus rendering the good faith exception inapplicable. (*Id.*).

I agree with the Sixth, Eighth and Tenth Circuits that suppression is not automatically warranted where evidence is seized pursuant to a warrant that is void *ab initio*.[12] *See Horton*, 863 F.3d at 1052 (concluding that *Leon* may apply to warrants that are void *ab initio*); *Workman*, 863 F.3d at 1319 ("[i]n our view, *Herring* and *Evans* govern, requiring application of the *Leon* exception when the search is based on a warrant exceeding the issuing judge's authority"); *United States v. Master*, 614 F.3d 236, 243 (6th Cir. 2010) (concluding that suppression is not automatically warranted under *Herring* where warrant is issued by judge who lacks authority); *see also United States v. Raymonda*, 780 F.3d 105, 118 n.5 (2d Cir.) ("the basic insight of the *Leon* line of cases that exclusion should be limited to cases of deliberate, reckless, or grossly-negligent disregard for Fourth Amendment rights applies equally to searches conducted with or without a warrant") (internal quotations and citation omitted), *cert. denied*, 136 S. Ct. 433 (2015). Consistent with the Supreme Court's decision in *Herring v. United States*, 555 U.S. 135 (2009), in determining whether to order suppression, a court should consider whether the benefits of deterrence outweigh the costs.

---

government's letter. (Docket # 57). Brooks responded to the government's letter on August 3, 2017. (Docket # 61).

[12] For purposes of this decision, the Court assumes, but does not decide, that the Rule 41(b) violation rendered the NIT warrant void *ab initio*; such a determination is ultimately unnecessary and would involve resolution of conflicting Circuit authority. *Compare Horton*, 863 F.3d at 1049 ("[t]he government argues that because the NIT warrant was proper in the Eastern District of Virginia, it cannot be wholly void or void *ab initio*[;] . . . [t]he possibility that the magistrate could have executed a proper warrant in the Eastern District of Virginia, however, does not save this warrant from its jurisdictional error"), *with Workman*, 863 F.3d at 1318 n.1 ("the warrant here was not void *ab initio*, for the warrant could validly be executed by extracting data from computers within the magistrate judge's district").

Of course, that the good faith exception *may* be applied to a warrant issued in violation of Rule 41 does not mean that it *should* apply to the NIT warrant at issue here. Rather, I must determine whether the agents acted in objective good faith reliance on the NIT warrant. *United States v. Leon*, 468 U.S. at 918-23 (Fourth Amendment exclusionary rule should not be applied to evidence obtained by a police officer whose reliance on a search warrant issued by a neutral magistrate was based on "objective good faith," even though the warrant itself might ultimately be found to be defective); *United States v. Salameh*, 152 F.3d 88, 114 (2d Cir. 1998), *cert. denied*, 525 U.S. 1112 (1999); *United States v. Benedict*, 104 F. Supp. 2d 175, 182 (W.D.N.Y. 2000). The rationale underlying this good faith exception is that the exclusionary rule "cannot be expected, and should not be applied, to deter objectively reasonable law enforcement activity." *Leon*, 468 U.S. at 919.

The Court in *Leon* identified four situations in which the good faith exception is inapplicable. Specifically, an executing officer's reliance on a search warrant will not be deemed to have been in good faith:

> (1) where the issuing magistrate has been knowingly misled;
>
> (2) where the issuing magistrate wholly abandoned his or her judicial role;
>
> (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and
>
> (4) where the warrant is so facially deficient that reliance upon it is unreasonable.

Id. at 923; *see United States v. Cancelmo*, 64 F.3d 804, 807 (2d Cir. 1995) (citations omitted). Accordingly, improperly obtained evidence may still be admissible so long as the executing agents acted "with an objectively 'reasonable good-faith belief' that their conduct [was] lawful

or when their conduct involve[d] only simple, isolated negligence." *Davis v. United States*, 564 U.S. 229, 238 (2011) (citations omitted) (quoting *Leon*, 468 U.S. at 919).

Brooks maintains that the good faith exception is inapplicable because the government's conduct in applying for the warrant was reckless and grossly negligent. (Docket ## 54 at 4-5; 61 at 2) (citing *United States v. Raymonda*, 780 F.3d at 118 ("[t]he Supreme Court has since clarified that the[] limitations [of *Leon*] apply not merely in cases of deliberate police misconduct, but also in situations where an officer is 'reckless' or 'grossly negligent' in seeking or executing a warrant")). According to Brooks, Alfin's testimony demonstrates that the warrant application was reviewed by many individuals, but not with respect to the geographical restrictions of Rule 41. (*Id.*). I disagree with Brooks's characterization of Alfin's testimony; in any event, his testimony demonstrates that the agents acted in objective good faith on the NIT warrant issued by the magistrate judge.

Alfin testified that he personally participated in drafting Macfarlane's affidavit and in meetings with other FBI agents and FBI and DOJ attorneys to discuss the warrant application. Brooks maintains that Alfin's testimony "showed that the government did not consider the restrictions of Rule 41 during the initial application and issuance of the warrant." (Docket # 54 at 4-5). To the contrary, Alfin did not testify that Rule 41 was not considered. Rather, he testified that he could not specifically recall whether Rule 41 was explicitly discussed during those meetings, but he was sure that during these meetings none of the attorneys expressed the opinion that the warrant was not authorized by Rule 41. According to Alfin, the general consensus was that the warrant was valid. Alfin testified that in addition to his own belief that the warrant was valid, he also relied upon the fact that the warrant had been reviewed

by several attorneys and his knowledge that similar warrants had been issued in other investigations.

Alfin's testimony demonstrates that the agents involved in the Playpen investigation acted thoughtfully and carefully in applying for the NIT warrant. They drafted a lengthy affidavit that explained the investigation, the technology at issue and the manner in which the NIT would operate, and that highlighted the anticipated geographical reach of the proposed warrant. Although Brooks maintains that the agents decided to "ignore the jurisdictional parameters of Rule 41" (Docket # 61), the record before the Court demonstrates that the agents executing the warrant relied in objective good faith on the validity of a warrant that had been reviewed by attorneys and approved by a magistrate judge.

Although I find that the magistrate judge lacked authority under Rule 41(b) to issue the NIT warrant, that absence of authority was not so apparent as to preclude a finding of objective good faith. Indeed, as noted above, many courts have reached the contrary conclusion that the issuing judge in fact had authority to issue the warrant under Rule 41(b)(4). Considering the complex legal issues implicated by this warrant, and the inconsistent determinations by different courts throughout the country, I agree with the majority of courts that have found that the executing agents acted in objective good faith in relying upon the validity of the NIT warrant. *See*, *e.g.*, *Horton*, 863 F.3d at 1052 ("[w]e, however, will not find an obvious deficiency in a warrant that a number of district courts have ruled to be facially valid[,] . . . [and] we . . . decline[] to impose an obligation on law enforcement to know the legal and jurisdictional limits of a judge's power to issue interstate search warrants") (internal quotations omitted); *Workman*, 863 F.3d at 1321 ("if a violation took place, it has escaped the notice of eight federal judges who have held that the same warrant complied with federal law and the federal rules even though data

was being extracted from computers outside the Eastern District of Virginia[;] . . . executing agents could reasonably have made the same mistake and reasonably relied on the magistrate judge's decision to issue the warrant"); *United States v. Hernandez-Cuellar*, 2017 WL 2297171 at *8 ("[t]he very fact that courts have split on the question of whether Rule 41(b) authorized the [issuing judge] to issue the NIT [w]arrant demonstrates that a reasonably well-trained officer could have concluded the NIT [w]arrant issued lawfully"); *Dorosheff*, 2017 WL 1532267 at *7 ("[c]ourts that have reviewed the NIT warrant are split as to whether the issuing magistrate had authority under Rule 41(b)[;] . . . [t]his split suggests that reasonable minds may disagree as to whether the magistrate had authority to issue the warrant"); *Taylor*, 2017 WL 1437511 at *16 ("[e]xclusion of the evidence seized pursuant to the NIT warrant would serve little deterrent purpose where the mistaken conduct of the magistrate judge, not the officers, invalidated the warrant"); *United States v. Schuster*, 2017 WL 1154088 at *9 ("the [c]ourt finds no basis to conclude that the . . . agents acted deliberately or recklessly in either obtaining or relying upon the NIT warrant[;] [r]ather, any deficiency in the NIT warrant was the result of judicial error, not law enforcement misconduct"); *Gaver*, 2017 WL 1134814 at *12 ("[t]o this [c]ourt's knowledge, every court within the Sixth Circuit that has been asked to suppress evidence obtained as a result of the NIT warrant has found that the good faith exception to the exclusionary rule applies[,] . . . [and] numerous courts outside of the Sixth Circuit have held that the good faith exception applies[;] . . . it cannot be said that Macfarlane's belief that the warrant was valid was objectively unreasonable"); *Perdue*, 237 F. Supp. 3d at 478-79 ("although this court has held that the NIT warrant violated Rule 41(b) by exceeding the magistrate judge's authority, the court also concludes that the government did not intentionally violate the Rule[;] [t]he court therefore concludes, as has nearly every other court to consider this question, that the good-faith exception

to the warrant applies to the execution of the NIT [w]arrant"); *United States v. Sullivan*, 229 F. Supp. 3d at 658 ("[a]ppying the balancing test required by Supreme Court and Sixth Circuit precedent, the [c]ourt finds that, even if the magistrate judge exceeded her jurisdiction, suppression is not warranted because the record before this [c]ourt demonstrates that the FBI agents acted with good faith by diligently gathering information before submitting a detailed affidavit that fully apprised the issuing magistrate judge of all aspects of the NIT process"). Any benefits of deterrence to be served by suppressing the evidence seized pursuant to the NIT warrant would be outweighed by the costs. *Herring*, 555 U.S. at 142. Accordingly, I recommend denial of Brooks's motion to suppress evidence seized pursuant to the NIT warrant.

II. Search of 116 Lexington Avenue and Brooks's Statements

Brooks also seeks to suppress evidence seized during the execution of a search warrant for his residence and the statements he made during that search on the grounds that they were the fruit of the unlawful NIT warrant. (Docket # 31 at 17-18, 20). Having concluded that suppression of the evidence seized pursuant to the NIT warrant is not appropriate, I likewise recommend that the district court deny this motion.

CONCLUSION

For the reasons stated above, I recommend that Brooks's motion to suppress tangible evidence and statements **(Docket ## 31, 54)** be **DENIED**.

s/Marian W. Payson
MARIAN W. PAYSON
United States Magistrate Judge

Dated: Rochester, New York
August 31, 2017

Pursuant to 28 U.S.C. § 636(b)(1), it is hereby

ORDERED, that this Report and Recommendation be filed with the Clerk of the Court.

ANY OBJECTIONS to this Report and Recommendation must be filed with the Clerk of this Court within fourteen (14) days after receipt of a copy of this Report and Recommendation in accordance with the above statute and Rule 59(b) of the Local Rules of Criminal Procedure for the Western District of New York.[13]

The district court will ordinarily refuse to consider on *de novo* review arguments, case law and/or evidentiary material which could have been, but was not, presented to the magistrate judge in the first instance. *See, e.g., Paterson-Leitch Co. v. Mass. Mun. Wholesale Elec. Co.*, 840 F.2d 985 (1st Cir. 1988).

Failure to file objections within the specified time or to request an extension of such time waives the right to appeal the District Court's Order. *Thomas v. Arn*, 474 U.S. 140 (1985); *Small v. Sec'y of Health & Human Servs.*, 892 F.2d 15 (2d Cir. 1989); *Wesolek v. Canadair Ltd.*, 838 F.2d 55 (2d Cir. 1988).

The parties are reminded that, pursuant to Rule 59(b) of the Local Rules of Criminal Procedure for the Western District of New York, "[w]ritten objections . . . shall specifically identify the portions of the proposed findings and recommendations to which objection is made and the basis for such objection and shall be supported by legal authority." **Failure to comply with the provisions of Rule 59(b) may result in the District Court's refusal to consider the objection.**

Let the Clerk send a copy of this Order and a copy of the Report and Recommendation to the attorneys for the parties.

IT IS SO ORDERED.

s/Marian W. Payson
MARIAN W. PAYSON
United States Magistrate Judge

Dated: Rochester, New York
August 31, 2017

[13] Counsel is advised that a new period of excludable time pursuant to 18 U.S.C. § 3161(h)(1)(D) commences with the filing of this Report and Recommendation. Such period of excludable delay lasts only until objections to this Report and Recommendation are filed or until the fourteen days allowed for filing objections has elapsed. *United States v. Andress*, 943 F.2d 622 (6th Cir. 1991); *United States v. Long*, 900 F.2d 1270 (8th Cir. 1990).